UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/701,404	11/03/2003	Benjamin Wilken	RIV-0490	6346

87555 7590 07/06/2009
Riverbed Technology Inc. - PVF
c/o Park, Vaughan & Fleming LLP
2820 Fifth Street
Davis, CA 95618

EXAMINER	
SQUIRES, BRETT S	
ART UNIT	PAPER NUMBER
2431	
MAIL DATE	DELIVERY MODE
07/06/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/701,404	**Applicant(s)** WILKEN ET AL.	
	Examiner BRETT SQUIRES	**Art Unit** 2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 April 2009*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4,6-11,14-17,19-31 and 33-40* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4,6-11,14-17,19-31, and 33-40* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

Claim Objections

1. Applicant is advised that should claims 1 and 8 be found allowable, claims 37-40 will be objected to under 37 CFR 1.75 as being a substantial duplicate thereof. The method of detecting scanning attacks recited by independent claim 1 states that "indicating a host as a scanner when at least one of the following conditions is true:," independent claim 1 then recites two conditions. Independent claim 37 recites the identical steps performed by independent claim 1 while omitting the second condition and independent claim 38 recites the identical steps performed by independent claim 1 while omitting the first condition. Accordingly, the methods of detecting scanning attacks recited by independent claims 37 and 38 are encompassed by the method of detecting scanning attacks recited by independent claim 1. The method detecting port scanning attacks recited by independent claim 8 states that "reporting a host associated with a port scan when at least one of the following condition is true:," independent claim 8 then recites two conditions. Independent claim 39 recites the identical steps performed by independent claim 8 while omitting the second condition and independent claim 40 recites the identical steps performed by independent claim 8 while omitting the first condition. Accordingly, the methods of detecting port scanning attacks recited by independent claims 39 and 40 are encompassed by the method of detecting port scanning attacks recited by independent claim 8. When two claims in an application are duplicates or else are so close in content that they both cover the same thing, despite a slight difference in wording, it is proper after allowing one claim to object to the other as being a substantial duplicate of the allowed claim. See MPEP § 706.03(k).

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-4, 6-11, 14-17, 19-31, 33-40 are rejected under 35 U.S.C. 103(a) as being obvious over Pruthi (US 2004/0015581) in view of Bruton et al. (US 7,222,366).

Regarding Claims 1, 14, 24, 28, and 37-38:

Pruthi discloses a method of detecting scanning attacks that adds host-pair connection records to a first data structure ("Host-Pairs Table" See fig. 14 ref. no. 1402 and paragraphs 115-116) stored on a computer readable medium ("Short-term Memory" and "Long-term Memory" See fig. 5 ref. nos. 508 and 510) when a host accesses another host during a first update period ("The start field specifies the beginning time from which the traffic is analyzed and its results are displayed on the GUI." and "The stop field specifies the ending time to which the traffic is analyzed and its results are displayed on the GUI." See paragraphs 92-93), determines the number of new host pairs added to the first data structure over the first update period ("The number of IP host pair connections involving a common IP address exceeds x over a time window y." See paragraph 187), aggregating host-pair connections records from the first data structure into a second data structure ("The records computed for time interval entered by the operator in the window field, such as 30 seconds, are aggregated over the time interval entered by the operator in the start and stop field, such as 2 hours." See fig. 10

ref. nos. 1013-1015 and paragraphs 92-94), and indicating a host as a scanner when the host appears in more than a first threshold number of host pairs within the first update period ("Providing a request for action in response to a pattern indicative of an intruder" See paragraphs 172-187), and a first historical number of host pairs is smaller than the first threshold by a first factor value (The examiner respectfully points out that it is inherent that the operator has access to the historical number of host pairs created by normal operating traffic over the network. The historical number is necessary for the method of detecting scanning attacks disclosed by Pruthi to function properly, as opposed to alerting the operator that the network is always under scanning attacks when normal operating traffic is on the network. See paragraph 200).

Pruthi does not disclose a second update period that is greater than the first update period, determining the number of new host pairs added to the second data structure over the second update period, and indicating a host as a scanner when the host appears in more than a second threshold number of host pairs within the second update period and a second historical number of host pairs is smaller than the second threshold number by a second factor value.

Bruton discloses an intrusion detection system for detecting scanning attacks that includes threshold values that define what constitutes a fast scanning attack and a slow scanning attack (See col. 8 lines 4-19).

It would have been obvious to one of ordinary skill in the art at the time of the invention to include in the method of detecting scanning attacks disclosed by Pruthi threshold values that define what constitutes a fast scanning attack and a slow scanning attack such as that taught by Bruton in order to improve intrusion detection (See Bruton col. 3 lines 36-51).

Regarding Claims 2, 15, 25, and 29:

The above stated combination of Pruthi and Bruton discloses user can configure the necessary parameters for threshold checking. This means that the x's and the y's as specified above are user-specifiable as well as other information need to define the threshold. (See Pruthi paragraph 200)

Regarding Claims 3, 16, 26, and 30:

The above stated combination of Pruthi and Bruton discloses the first data structure is a current time-slice connection table and host-pair connection records are added to the current time slice connection table ("The connection table is continuously updated at the time interval indicated by the operator in the window field when the operator has indicated that the connection table should be continuously updated in the stop field." See Pruthi fig. 10 ref. nos. 1014-1015 and paragraphs 93-94).

Regarding Claims 4, 17, 27, and 31:

The above stated combination of Pruthi and Bruton discloses checking for ping scans at the end of the second update period ("The method of detecting scanning attacks keeps track of ICMP echo request packets." See Pruthi paragraph 219) and indicating hosts which produced more than the second threshold of new host pairs over the second update period ("When the number of ping scans detected exceeds the threshold x, the difference between the numbers of ping scans detected and the threshold x corresponds to 'C3'." See paragraph 187).

Regarding Claims 6 and 19:

The above stated combination of Pruthi and Bruton discloses maintaining Address Resolution Protocol packet statistics in the first data structure and for sparse subnet tracking the number of generated ARP requests that do not receive response to detect scans on sparse sub-networks ("The examiner respectfully points out that method for detecting scanning attacks can be implement on spare sub-networks." See Pruthi paragraphs 35, 42, 109, and 202).

Regarding Claim 7:

The above stated combination of Pruthi and Bruton discloses the scanning attack is a ping scanning attack ("The method of detecting scanning attacks keeps track of ICMP echo request packets." See Pruthi paragraph 219)

Regarding Claims 8, 20, 33, and 39-40:

Pruthi discloses a method of detecting scanning attacks that retrieves from a first data structure ("Host-Pairs Table" See fig. 14 ref. no. 1402 and paragraphs 115-116) stored on a computer readable medium ("Short-term Memory" and "Long-term Memory" See fig. 5 ref. nos. 508 and 510) logged values of protocols and ports in host-pair connections records added in the first data structure during a first update period ("The start field specifies the beginning time from which the traffic is analyzed and its results are displayed on the GUI." and "The stop field specifies the ending time to which the traffic is analyzed and its results are displayed on the GUI." See paragraphs 92-93), determines the number of ports associated with a host over the first update period based on the host pair-connection records in the first data structure ("The number of IP host pair connections involving a common IP address exceeds x over a time window y." See paragraph 187), aggregates host-pair connection records from the first data structure into a second data structure ("The records computed for time interval entered by the operator in the window field, such as 30 seconds, are aggregated over the time interval entered by the operator in the start and stop field, such as 2 hours." See fig. 10 ref. nos. 1013-1015 and paragraphs 92-94), reporting a host associated with a port scan when the number of ports associated with the host within the first update period is greater than a first threshold number ("Providing a request for action in response to a pattern indicative of an intruder" See paragraphs 172-187) and a first historical number of ports associated with the host is smaller than the first threshold number by a first factor value (The examiner respectfully points out that it is inherent that the operator has access to the historical number of host pairs created by normal operating traffic over the network. The historical number is necessary for the method of detecting scanning attacks disclosed by Pruthi to function properly, as opposed to alerting the operator that the network is always under scanning attacks when normal operating traffic is on the network. See paragraph 200).

Pruthi does not discloses a second update period that is greater than the first update period, determining the number of ports associated with a host over the second update period based on the host-pair connection records in the second data structure, reporting a host associated with a port scan when the number of ports associated with the host within the second update period is greater than a second threshold number, and a second historical number of ports associated with the host is smaller than the second threshold number by a second factor value.

Bruton discloses an intrusion detection system for detecting scanning attacks that includes threshold values that define what constitutes a fast scanning attack and a slow scanning attack (See col. 8 lines 4-19).

It would have been obvious to one of ordinary skill in the art at the time of the invention to include in the method of detecting scanning attacks disclosed by Pruthi threshold values that define what constitute a slow scanning attack such as that taught by Bruton in order to improve intrusion detection (See Bruton col. 3 lines 36-51).

Regarding Claims 9, 21, and 34:

The above stated combination of Pruthi and Bruton discloses assigning a severity level to the port scan and reporting the severity level of the port scan ("The present invention allows specification of a 'sensitivity level' and 'suspicion level' which will determine whether certain events are counted toward a scan event threshold, based on the circumstance surrounding the event." See Bruton col. 15 lines 7-35).

Regarding Claims 10, 22, and 35:

The above stated combination of Pruthi and Bruton discloses the reported severity varies as a function of the deviation from the historical norm ("The historical norm is selected to be below threshold x, so when the number of ports being scanned is larger the threshold x the number of ports deviates from the historical norm." See Pruthi paragraphs 187 and 199-209).

Regarding Claims 11, 23, and 36:

The above stated combination of Pruthi and Bruton discloses determining from accessing data in the connection table statistics about TCP reset packets ("Once a packet is identified as TCP the packet is then examined to determine whether it opens or is initiating a TCP connection." See Pruthi paragraphs 67-68) and ICMP port-unreachable packets ("The network monitor is able to analyze ICMP traffic and ICMP port unreachable packets are included in ICMP traffic." See Pruthi paragraph 35), to detect a spike in the number of reset packets and ICMP port-unreachable packets relative to the historical profile to increase the severity of a port scan event (See Pruthi paragraphs 35, 114, 165, and 219).

Conclusion

4. Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRETT SQUIRES whose telephone number is (571) 272-8021. The examiner can normally be reached on 9:30am - 6:00pm Monday - Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on (571) 272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BS/

/William R. Korzuch/
Supervisory Patent Examiner, Art Unit 2431